

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/832,511	04/10/2001	Timothy S. Collins	ERX1P003	2459
32137	7590	08/04/2004	EXAMINER	
COWAN, LIEBOWITZ & LATMAN, P.C. 1133 AVENUE OF THE AMERICAS NEW YORK, NY 10036			SHIFERAW, ELENI A	
			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 08/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/832,511

Applicant(s)

COLLINS ET AL.

Examiner

Eleni A Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 10 April 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☒ Claim(s) 20 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

1. Claims 1-20 are presented for examination.

#### ***Specification***

2. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

#### ***Claim Objections***

3. Claim 20 is objected to because of the following informalities: it is unclear what "at the" is claiming on line 26. Appropriate correction is required.

Art Unit: 2136

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-2, 4-9 are rejected under 35 U.S.C. 102(b) as being anticipated by Arnold (PN US 5,787,172).

6. As per claim 1, Arnold teaches a method of forming a certificate, comprising:  
placing a first public key of a first encryption type in the certificate (Col. 6 lines 22-46);  
and  
placing a second public key of a second encryption type in the certificate (Col. 6 lines 22-46).

7. As per claim 2, Arnold teaches the method, wherein the second public key is placed as at least one extension of the certificate (Col. 6 lines 22-46).

8. As per claim 4, Arnold teaches the method, wherein the extension where the second public key is placed specifies a key type (Col. 33 lines 50-col. 34 lines 19), a key length (Col. 25 lines 19-45), and a key value (Col. 25 lines 19-45, col. 17-lines 1-16).

9. As per claim 5, Arnold teaches the method, wherein the placing of the first public key and the placing of the second public key places the first and second public keys in a certificate information string, where the extension is part of the certificate information string and further comprising:

Art Unit: 2136

creating a signature from the certificate information string (Col. 10 lines 56-67); and  
adding the signature to the certificate information string to form the certificate (Col. 4  
lines 48-67).

10. As per claim 6, Arnold teaches the method, further comprising:

placing a hashing algorithm in the certificate information string, wherein the hashing  
algorithm is used to create the signature (Col. 38 lines 5-32); and

placing a certificate authority identifier, which identifies a certificate authority,  
in the certificate information string (Col. 38 lines 5-37).

11. As per claim 7, Arnold teaches the method, wherein a private key of the certificate  
authority is used to generate the signature (Col. 10 lines 56-67).

12. As per claim 8, Arnold teaches the method, wherein the placing of the first public key  
and the placing of the second public key places the first and second public keys in a certificate  
information string and further comprising:

creating a signature from the certificate information string (Col. 10 lines 56-67); and  
adding the signature to the certificate information string to form the certificate (Col. 4  
lines 48-67).

13. As per claim 9, Arnold teaches the method, further comprising:

placing a hashing algorithm in the certificate information string, wherein the hashing  
algorithm is used to create the signature (Col. 38 lines 5-32); and

placing a certificate authority identifier, which identifier a certificate authority,

Art Unit: 2136

in the certificate information string (Col. 38 lines 5-37), wherein a private key of the certificate authority is used to generate the signature (Col. 10 lines 56-67).

14. Claims 10-11, 13, 15, 18, and 19 rejected under 35 U.S.C. 102(b) as being anticipated by Spelman et al. (Spelman, PN 5,764,768).

15. As per claim 10, Spelman teaches a method, method for transmitting a document comprising digitally signing the document, comprising:

encrypting an information string with a private key to create a signature (Col. 7 lines 7-16), wherein the private key is related to a public key in a certificate (Col. 1 lines 57-67), wherein the certificate comprises a first public key and a second public key (Col. 1 lines 57-67), wherein the public key related to the private key is the second public key (Col. 1 lines 57-67) and wherein the information string contains the document (Col. 7 lines 7-16); and

attaching the signature to the information string to create a digitally signed document (Col. 7 lines 7-16).

16. As per claim 11, Spelman teaches the method, wherein the first public key is a first encryption type and the second public key is a second encryption type, which is different from the first encryption type (Col. 1 lines 56-67).

17. As per claim 13, Spelman teaches the method, wherein the second public key is placed in an extension of the certificate (Col. 3 lines 39-59).

Art Unit: 2136

18. As per claim 15, Spelman teaches the method, further comprising hashing the information string, so that the encrypting of the information string encrypts the hashed information string (Col. 7 lines 6-24).
19. As per claim 18, Spelman teaches the method, further comprising:  
transmitting the digitally signed document from a first device (Col. 6 lines 1-26, Fig. 2B, 3); and  
receiving the digitally signed document at a second device (Col. 6 lines 19-35, Fig. 3).
20. As per claim 19, Spelman teaches the method, wherein the certificate is the certificate for the first device, further comprising:  
obtaining the second public key from an extension of the certificate for the first device (Col. 3 lines 39-59); and  
using the second public key to verify the digitally signed document (Col. 7 lines 16-24).

***Claim Rejections - 35 USC § 103***

21. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

22. Claims 14, 16, 17 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spelman et al. (Spelman, PN US 5,764,768) in view of Arnold (PN US 5,787,172).



23. As per claim 14, Spelman and Arnold teach all the subject matter as described above.

Spelman fail to explicitly teach adding text to digitally signed document to specify the location of the second public key,

However Arnold teaches the trusted authority generating a cryptographic data element that comprises any information that can be used to establish a cryptographic link (Col. 25 lines 20-45)

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Arnold with in the system of Spelman because adding text to digitally signed document would specify the certificate clearly. The information may inform what the index number is, what an identifier or serial number is, what a secret key or an encryption key is. (Col. 25 lines 20-45). It is obvious to add text information to specify the location of the second public key because the text information would clearly specify where the second public key is located in the certificate.

24. As per claim 16, Spelman teaches all the subject matter as described above.

Spelman fails to explicitly teach a key type, a key length, and a key value,

However Arnold teaches the method, wherein the extension where the second public key is placed specifies a key type (Col. 33 lines 50-col. 34 lines 19), a key length (Col. 25 lines 19-45), and a key value (Col. 25 lines 19-45, col. 17-lines 1-16).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Arnold with in the system of Spelman because it would clarify what type of key is used, the length of the key, and a key value; and

provide a secure, and relatively inexpensive cryptographic system (Col. 3 lines 40-52). The trusted authority generates a cryptographic data element that comprises any information to establish a cryptographic link. For example, the data element may comprise an index or seed, an identifier or serial number, and a secret key or an encryption key (Col. 25 lines 20-45).

25. As per claim 17, Spelman teaches the method, wherein the certificate further comprises an issuer name (Col. 7 lines 17-34), and a subject name (Col. 7 lines 17-34),

Spelman do not explicitly teach a validity range,

However Arnold teaches a validity range used in digital certificate,

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Arnold with in the system of Spelman because it would allow to performs the signature verification by checking the effective date and expiration date obtained form the authentication certificate in which the certificate is valid. If the signature verification is successful, and the secure chip advances to the process block, the secure chip will then check the content of the authorization data value contained in the authentication certificate. The secure chip will compare the effective date and the expiration date obtained from the authentication certificate against the manufacturing date code contained in the ROM of the secure chip. At a decision block, the secure chip determines whether the authentication certificate is fresh. A certificate or message is fresh if its manufacturing date code falls between the effective date and the expiration date of the certificate or the message (Col. 17 lines 56- col. 18 lines 20). Therefore it is obvious to have a certificate that comprises a validity range.

Art Unit: 2136

26. As per claim 20, Spelman and Arnold teach all the subject matter as described above.

Spelman fail to explicitly receiving at the second device instructions designating the location of the second public key,

However Arnold teaches receiving a cryptographic data element comprising an initial key package (IKP) (Col. 25 lines 20-52)

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Arnold with in the system of Spelman because the cryptographic data element that comprises an IKP will contain cryptographic information that is required to inform the receiver at the second device(Col. 25 lines 20-52). It is obvious to receive instructions to designate the location of the second public key because the text information would specify where the second public key is located in the certificate.

27. Claims 3 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spelman et al. (Spelman, PN US 5,764,768) in view of Arnold (PN US 5,787,172), and in further view of Crandall et al. (Crandall, PN US 6,307,935 B1)

28. As per claims 3 and 12, Spelman and Arnold teach all the subject matter as described above.

Spelman and Arnold do not explicitly teach the second encryption type is faster than the first encryption type teaches,

However Crandall teaches the method of fast elliptic encryption to encrypt plain text (Col. 9 lines 31-49, col. 14 lines 27-35) to generate digital signature (Fig. 10).

Therefore it would have been obvious to one having ordinary skill in the art at the time

the invention was made to employ the teachings of Crandall with in the combination of Spelman and Arnold because it would perform fast arithmetic to improve problems of RSA when factoring very large prime numbers. The method provides means for encrypting plaintext directly as points on elliptic curves. The ease of embedding in the method is a result of choosing elliptic curve parameterizations over a field  $F_{p^2}$ , where  $p$  is a prime number such that  $p \equiv 3 \pmod{4}$ . The integers  $q$  and  $C$  are chosen such that  $p$  be prime, with  $C$  (possibly negative) being suitably small in magnitude so that fast arithmetic can be performed (Col. 5 lines 49-57).

29. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 703-305-0326. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Application/Control Number: 09/832,511

Page 11

Art Unit: 2136

Eleni Shiferaw

Art Unit 2136

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100